TRAITÉ DE COOPERATION EN MATIÈRE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Destinataire:

NONNENMACHER, Bernard
Gemplus
Parc d'Activités de Gémenos
Avenue du Pic de Bertagne
F-13881 Gémenos Cedex
FRANCE

Date d'expédition (jour/mois/année)
02 octobre 2000 (02.10.00)

Référence du dossier du déposant ou du mandataire
GEM 628

NOTIFICATION IMPORTANTE

Demande internationale no
PCT/FR99/02782

Date du dépôt international (jour/mois/année)
12 novembre 1999 (12.11.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

[X] le déposant [ ] l'inventeur [ ] le mandataire [ ] le représentant commun

Nom et adresse

GEMPLUS S.C.A.
Parc d'Activités de Gémenos
Avenue du Pic de Bertagne
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat): FR
Domicile (nom de l'Etat): FR
no de téléphone:
no de télécopieur:
no de téléimprimeur:

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

[ ] la personne [X] le nom [ ] l'adresse [ ] la nationalité [ ] le domicile

Nom et adresse

GEMPLUS
Parc d'Activités de Gémenos
Avenue du Pic de Bertagne
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat): FR
Domicile (nom de l'Etat): FR
no de téléphone:
no de télécopieur:
no de téléimprimeur:

3. Observations complémentaires, le cas échéant:
Ce changement s'applique également à l'adresse du mandataire, comme indiqué dans le cadre destinataire ci-dessus.

4. Une copie de cette notification a été envoyée:

[X] à l'office récepteur
[ ] à l'administration chargée de la recherche internationale
[ ] à l'administration chargée de l'examen préliminaire international
[ ] aux offices désignés concernés
[X] aux offices élus concernés
[ ] autre destinataire:

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:
Yolaine CUSSAC

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 20 juin 2000 (20.06.00)	
Demande internationale no PCT/FR99/02782	**Référence du dossier du déposant ou du mandataire** GEM 628
Date du dépôt international (jour/mois/année) 12 novembre 1999 (12.11.99)	**Date de priorité** (jour/mois/année) 18 novembre 1998 (18.11.98)
Déposant VALADIER, Jean-Louis	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

19 mai 2000 (19.05.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

R. Forax

no de téléphone: (41-22) 338.83.38

Translation
09/856269

7

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM 628	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/02782	International filing date (*day/month/year*) 12 November 1999 (12.11.99)	Priority date (*day/month/year*) 18 November 1998 (18.11.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
19 May 2000 (19.05.00)	10 August 2000 (10.08.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

International application No.
PCT/FR99/02782

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-14, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 1-12, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/4-4/4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-12	YES
	Claims		NO
Inventive step (IS)	Claims	1-12	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

2. Citations and explanations

Document EP-A-481882 (D1) is considered to be the closest prior art.

D1 discloses (see Claim 1, and Figure 1) a method for controlling the use of a smart card, which comprises a microprocessor capable of performing cryptography calculations in the card, to carry out authentication sessions during a transaction between the card and a terminal. The aforementioned method uses at least one control counter (sum box) and, for a transaction including at least one authentication session by the card, consists in decrementing or incrementing the control counter by one unit, at the beginning of the transaction, and if the card authentication succeeds, clearing the counter of the bits.

The subject matter of Claim 1 differs from the prior art only in that the counter is not reset, but is decremented by one unit.

In comparison to Document D1, this method limits attacks of the DPA (Differential Power Analysis) kind.

Document EP-A-789335 envisages the use of a counter that

can increment or decrement in an irreversible way when authentication is not successful. This method is likewise not adapted to resist an attack of the DPA kind (see the description of the present application, pages 3 and 4).

Given that no single document made available to the examiner discloses resetting the counter when authentication is successful, the subject matter of Claim 1 is considered inventive.
The provisions of PCT Article 33 are, therefore, fulfilled.

With respect to the subject matter of Claim 12, the attention of the applicant is drawn to Box VIII below.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Contrary to the requirements of PCT Rule 5.1(a)(ii), the relevant prior art disclosed in document EP-A-481882 is not indicated in the description, nor is this document cited therein.

Claim 1 has not been drafted in the two-part form according to PCT Rule 6(3). Features known from D1 are included in the characterising part, whereas they should be included in the preamble.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claim 12 is not clear and does not meet the requirements of PCT Article 6 because the subject matter for which protection is sought is not clearly defined.
In particular, the technical features enabling the card to implement the methods previously defined are neither defined nor included in this claim.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 628	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 99/ 02782	Date du dépôt international *(jour/mois/année)* 12/11/1999	(Date de priorité (la plus ancienne) *(jour/mois/année)* 18/11/1998
Déposant GEMPLUS S.C.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 2 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la langue, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne les séquences de nucléotides ou d'acides aminés divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le titre,

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'abrégé,

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n° 2

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [X] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/02782

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de donnée électronique consultée au cours de la recherche internationale (nom de la base de donnée, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 789 335 A (DEUTSCHE TELEKOM) 13 août 1997 (1997-08-13)	1,2
A	le document en entier	9
Y	EP 0 481 882 A (GEMPLUS CARD INTERNATIONAL) 22 avril 1992 (1992-04-22) abrégé; revendications; figures	1,2
A	GB 2 188 762 A (P.H. BERTENSHAW) 7 octobre 1987 (1987-10-07) le document en entier	1-5,9-11
A	EP 0 626 662 A (GEMPLUS CARD INTERNATIONAL) 30 novembre 1994 (1994-11-30)	
A	EP 0 157 303 A (TOSHIBA) 9 octobre 1985 (1985-10-09)	

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 février 2000	06/03/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 99/02782

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0789335	A	13-08-1997	DE 19604349	A	14-08-1997
EP 0481882	A	22-04-1992	FR 2668278	A	24-04-1992
			CA 2053740	A,C	20-04-1992
			DE 69101099	D	10-03-1994
			DE 69101099	T	07-07-1994
			ES 2059085	T	01-11-1994
			JP 4264688	A	21-09-1992
			JP 7066431	B	19-07-1995
			US 5296687	A	22-03-1994
GB 2188762	A	07-10-1987	AUCUN		
EP 0626662	A	30-11-1994	FR 2705810	A	02-12-1994
			DE 69419967	D	16-09-1999
			DE 69419967	T	09-12-1999
			US 5550919	A	27-08-1996
EP 0157303	A	09-10-1985	JP 60207957	A	19-10-1985
			US 4879645	A	07-11-1989

TRAITE D OOPERATION EN MATIER DE BREVETS

16T

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 628	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02782	Date du dépot international *(jour/mois/année)* 12/11/1999	Date de priorité *(jour/mois/année)* 18/11/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07F7/10		
Déposant GEMPLUS S.C.A. et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

I	☒	Base du rapport
II	☐	Priorité
III	☐	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
IV	☐	Absence d'unité de l'invention
V	☒	Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
VI	☐	Certains documents cités
VII	☒	Irrégularités dans la demande internationale
VIII	☒	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
19/05/2000	10.08.00
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Closa, D N° de téléphone +49 89 2399 2880

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02782

I. Base du rapp rt

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.*) :

Description, pages:

1-14 version initiale

Revendications, N°:

1-12 version initiale

Dessins, feuilles:

1/4-4/4 version initiale

2. Les modifications ont entrainé l'annulation :

☐ de la description, pages :

☐ des revendications, n^{os} :

☐ des dessins, feuilles :

3. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications 1-12
	Non :	Revendications
Activité inventive	Oui :	Revendications 1-12
	Non :	Revendications
Possibilité d'application industrielle	Oui :	Revendications 1-12
	Non :	Revendications

2. Citations et explications

voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :

voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :

voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Le document EP-A-481882 (D1) est considéré comme représentant l'état de la technique le plus proche.

D1 montre (voir la revendication 1 et la figure 1) un procédé de contrôle de l'utilisation d'une carte à puce comprenant un microprocesseur apte à effectuer des calculs de cryptographie dans la carte pour effectuer des sessions d'authentification lors d'une transaction entre la carte et un terminal, ledit procédé utilise au moins un compteur de contrôle (zone totalisatrice) et consiste pour une transaction comprenant au moins une session d'authentification par la carte à décrémenter ou incrémenter d'une unité le compteur de contrôle au début de la transaction et si l'authentification par la carte est réussie d'effacer les bits du compteur.

L'objet de la revendication 1 ne diffère uniquement de l'état de la technique qu'en ce que le compteur n'est pas remis dans son état initial mais décrémenté d'une unité.

Par rapport au document D1, ce procédé permet de limiter des attaques de type DPA (Differential Power Analysis)

Le document EP-A-789335 prévoit l'utilisation d'un compteur s'incrémentant ou se décrémentant de façon irréversible lorsque l'authentification n'est pas réussie. Cette méthode n'est pas non plus adaptée pour résister à une attaque de type DPA, voir la description de la présente demande, pages 3 et 4.

Compte tenu qu'aucun des documents mis à la disposition de l'examinateur ne dévoile la remise du compteur dans son état initial lorsque l'authentification est réussie, l'objet de la revendication 1 est considéré comme inventif.
Les dispositions de l'Art. 33 PCT sont donc remplies.

En ce qui concerne l'objet de la revendication 12, l'attention du demandeur est attirée sur le point VIII, ci-dessous.

Concernant le point VII

Irrégularités dans la demande internationale

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans le document EP-A-481882 et ne cite pas ce document.

La revendication 1 n'est pas correctement découpée en deux parties comme requis par la règle 6(3) PCT. Des caractéristiques connues de D1 étant actuellement placées dans la partie caractérisante alors qu'elles devraient être dans le préambule.

Concernant le point VIII

Observations relatives à la demande internationale

La revendication 12. n'est pas claire et ne satisfait pas aux conditions requises à l'article 6 PCT, dans la mesure où l'objet pour lequel une protection est demandée n'est pas clairement défini.
En particulier, les caractéristiques techniques qui permettraient à la carte de mettre en oeuvre les procédés précédemment définis ne sont pas défini ne sont pas inclus dans cette revendication.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G07F 7/10	A1	(11) Numéro de publication internationale: WO 00/30049
		(43) Date de publication internationale: 25 mai 2000 (25.05.00)

(21) Numéro de la demande internationale: PCT/FR99/02782

(22) Date de dépôt international: 12 novembre 1999 (12.11.99)

(30) Données relatives à la priorité:
98/14497 18 novembre 1998 (18.11.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F–13881 Gémenos Cedex (FR).

(71)(72) Déposant et inventeur: VALADIER, Jean–Louis [FR/FR]; 22, impasse Omphale, F–13011 Marseille (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR CONTROLLING THE USE OF A SMART CARD

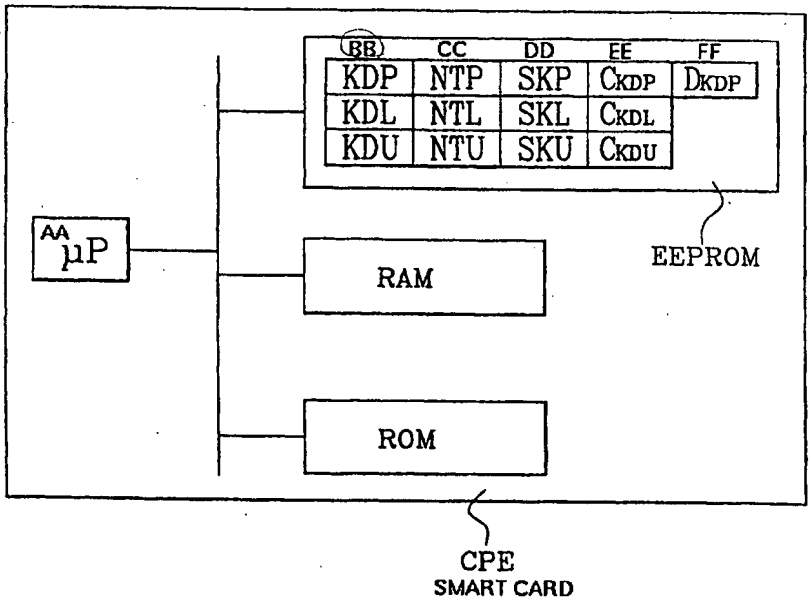
(54) Titre: PROCEDE DE CONTROLE D'UTILISATION D'UNE CARTE A PUCE

(57) Abstract

The invention concerns a method for controlling in a smart card CPE, for transactions between said card and a terminal comprising at least an authentication session by the card which consists in decrementing, or incrementing, by one unit control counter C_{KDP} at the start of the transaction and in re–incrementing it, or decrementing it, only if the authentication by the card is successful. When the counter reaches a threshold value, the use of the card is blocked, thereby preventing fraudulent use of the card in an attempt to discover the encryption keys KDP, SKP contained in the card.

(57) Abrégé

Un procédé de contrôle dans une carte à puce CPE, pour des transactions entre cette carte et un terminal comprenant au moins une session d'authentification par la carte consiste à décrémenter, ou incrémenter, d'une unité un compteur de contrôle C_{KDP} au début de la transaction et à ne le ré–incrémenter, ou le décrémenter, que si l'authentification par la carte est réussie. Lorsque le compteur atteint une valeur limite, l'utilisation de la carte est bloquée. De cette manière on empêche



AA...MICROPROCESSOR
BB...SECRET KEYS
CC...ASSOCIATED SESSION COUNTERS
DD...ENCRYPTION KEYS
EE...ASSOCIATED CONTROL COUNTER
FF...CHECK COUNTER

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie
AM	Arménie
AT	Autriche
AU	Australie
AZ	Azerbaïdjan
BA	Bosnie-Herzégovine
BB	Barbade
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BJ	Bénin
BR	Brésil
BY	Bélarus
CA	Canada
CF	République centrafricaine
CG	Congo
CH	Suisse
CI	Côte d'Ivoire
CM	Cameroun
CN	Chine
CU	Cuba
CZ	République tchèque
DE	Allemagne
DK	Danemark
EE	Estonie
ES	Espagne
FI	Finlande
FR	France
GA	Gabon
GB	Royaume-Uni
GE	Géorgie
GH	Ghana
GN	Guinée
GR	Grèce
HU	Hongrie
IE	Irlande
IL	Israël
IS	Islande
IT	Italie
JP	Japon
KE	Kenya
KG	Kirghizistan
KP	République populaire démocratique de Corée
KR	République de Corée
KZ	Kazakstan
LC	Sainte-Lucie
LI	Liechtenstein
LK	Sri Lanka
LR	Libéria
LS	Lesotho
LT	Lituanie
LU	Luxembourg
LV	Lettonie
MC	Monaco
MD	République de Moldova
MG	Madagascar
MK	Ex-République yougoslave de Macédoine
ML	Mali
MN	Mongolie
MR	Mauritanie
MW	Malawi
MX	Mexique
NE	Niger
NL	Pays-Bas
NO	Norvège
NZ	Nouvelle-Zélande
PL	Pologne
PT	Portugal
RO	Roumanie
RU	Fédération de Russie
SD	Soudan
SE	Suède
SI	Slovénie
SK	Slovaquie
SN	Sénégal
SZ	Swaziland
TD	Tchad
TG	Togo
TJ	Tadjikistan
TM	Turkménistan
TR	Turquie
TT	Trinité-et-Tobago
UA	Ukraine
UG	Ouganda
US	Etats-Unis d'Amérique
UZ	Ouzbékistan
VN	Viet Nam
YU	Yougoslavie
ZW	Zimbabwe

PROCÉDÉ DE CONTROLE D'UTILISATION D'UNE CARTE A PUCE

La présente invention concerne un procédé de contrôle d'une carte à puce.

Elle s'applique plus particulièrement aux cartes mettant en oeuvre des algorithmes de cryptographie utilisant des clés ou des couples de clés dans des sessions d'authentification, lors de transactions entre la carte et un terminal.

On entend par terminal, aussi bien le terminal dans lequel la carte est introduite, comme par exemple un terminal de paiement chez un commerçant, qu'un serveur d'une banque auquel ce terminal de paiement peut-être relié lors d'une transaction dite par liaison directe, selon un mode de transaction dit "*online*" dans la littérature anglo-saxonne. C'est notamment le cas pour les cartes bancaires (carte de débit/crédit), pour des transactions portant sur un montant qui dépasse un certain seuil et dans lesquelles le terminal se connecte automatiquement au serveur pour des vérifications supplémentaires avant d'accepter la transaction.

Dans la suite, on entend par terminal tout système extérieur auquel la carte est connectée lors d'une transaction.

L'invention s'applique notamment, mais pas exclusivement aux cartes à puce de type porte-monnaie électronique, qui sont des moyens de paiement jetables ou rechargeables.

Pour prévenir toute fraude liée à l'utilisation de cartes à puce, des algorithmes cryptographiques sont utilisés, qui utilisent des clés.

En pratique, pour un certain nombre de transactions une ou plusieurs sessions d'authentification par la carte ou par le terminal sont prévues , de manière à assurer une sécurité maximum. On entend par session d'authentification l'ensemble des opérations visant à faire calculer par la carte et par le terminal une signature (ou un certificat) correspondant à l'application d'un algorithme de cryptographie sur une donnée qui peut-être imposée par l'un ou l'autre ou un mélange de données de la carte et du terminal, et à la comparaison des deux signatures. Si cette comparaison est effectuée par la carte, c'est une authentification par la carte, qui reçoit la signature calculée par le terminal. Si c'est une authentification par le terminal, c'est le contraire.

Cependant, un nouveau type de fraude est apparue qui consiste à déduire la valeur des clés secrètes à partir d'analyses statistiques basées sur des mesures de consommation en courant de la carte, lors des périodes de calcul cryptographique. Cette méthode d'attaque, appelée attaque DPA pour *differential power analysis* repose sur le fait que l'on a des signatures de consommation en courant à partir desquelles, si on connaît au moins la donnée appliquée en entrée ou la donnée obtenue en sortie, on est capable, en faisant des hypothèses sur les clés, de retrouver la valeur ou une partie de la valeur d'une clé qui a été utilisée dans le calcul cryptographique considéré.

Pour mettre en oeuvre cette fraude, il faut donc pouvoir lancer un calcul cryptographique avec la même clé un certain nombre de fois, par exemple, 300 fois. Pour que ce soit utilisable, il faut connaître ou pouvoir imposer ou pouvoir fixer un paramètre du calcul cryptographique.

Si on prend l'exemple des cartes à puce de type porte-monnaie électronique mettant en oeuvre un

algorithme de cryptographie à clé secrète, les transactions entre une carte de ce type et un terminal se déroulent globalement selon le schéma suivant, représenté sur la figure 1 :

- dans une phase d'initialisation, la carte calcule une clé de session SKX, à partir d'une clé secrète KDX contenue dans la carte concernée et d'un compteur de sessions NTX de la carte qui est incrémenté de façon irréversible pendant la transaction.

Puis selon le type de transactions, la carte calcule une signature S1 et/ou une signature S2, en appliquant l'algorithme de cryptographie à une donnée, en général imposée par la carte, et avec la clé de session SKX.

De son côté, le terminal calcule des signatures correspondantes, et selon le type de transaction, soit le terminal est authentifié par la carte, soit la carte est authentifiée par le terminal. Il y a donc transmission de données et de signatures associées lors de sessions d'authentification.

Prenons le cas d'une tentative de fraude basée sur une transaction de type chargement (*load dans la littérature anglo-saxonne*), qui sert normalement à créditer la carte de type porte-monnaie électronique avec une certaine somme.

Si on lance un certain nombre de fois (300 fois par exemple) une transaction de ce type et si on retire la carte du terminal juste après la phase d'initialisation, le compteur de sessions NTX de la carte ne sera pas incrémenté. Si on fait 300 transactions de ce type en retirant la carte du terminal pour faire avorter la transaction, la clé de session SKX sera la même pour ces 300 transactions. On pourra donc collecter 300 courbes de mesure de consommation en courant correspondant au calcul de 300 signatures sur des données qui pourront être identiques

ou variables selon les transactions, et avec la même clé.

L'analyse statistique dans le cas où les données sur lesquelles le calcul cryptographique est appliqué, sont variables, permet d'obtenir la clé de session.

Selon le type de cartes, selon les transactions, on peut en pratique soit déduire les clés secrètes réelles contenues dans la carte, ou les clés de session.

La connaissance d'une clé secrète réelle permet d'une part de fabriquer des fausses cartes avec cette clé ; ces cartes seront vues comme bonnes par un terminal. Cette connaissance permet d'autre part de réaliser des transactions de type annulation d'achat, pour une carte de type porte-monnaie, permettant de re-créditer la carte d'un montant précédemment débité.

La connaissance d'une clé de session permet quant à elle de rejouer une transaction, en utilisant une fausse carte (un clone) ou un simulateur.

L'invention a pour objet d'empêcher ce type de fraude.

Or cette fraude nécessite deux type d'opérations distinctes:

- une opération de collection de mesures de consommation en courant, pour laquelle il faut utiliser la carte pour faire les mesures à des moments propices, avec des transactions réelles avec un terminal, mais qui sont avortées par retrait de la carte (*pull out*) ou des transactions avec un simulateur du terminal, transactions qui vont échouées par défaut d'authentification du terminal par la carte (mauvaises signatures) ; et

- une opération d'analyse statistique utilisant des moyens de simulation (ordinateurs), pour retrouver les données recherchées, c'est à dire les clés.

Pour mener à bien l'analyse statistique, il faut effectuer un grand nombre de mesures : 50, 300, 5000.

Cela veut dire que dans la carte, il va y avoir un grand nombre d'échecs de sessions d'authentifications par la carte, échecs dûs à des transactions avortées, par retrait de la carte du terminal (*pull-out*) ou échouées, par fourniture par le terminal de mauvaises signatures mauvaises signatures.

Un objet de l'invention est ainsi d'empêcher la collection de mesures de consommation en courant.

Or on a vu que dans le cas où l'on cherche à faire cette collection, on va avoir un grand nombre d'échecs de sessions d'authentification par la carte.

Une solution apportée au problème technique de l'invention consiste à utiliser dans la carte un compteur de contrôle, pour décompter (ou compter) ces échecs, et interdire l'utilisation de la carte quand un certain nombre d'échecs sont comptabilisés.

L'invention concerne donc un procédé de contrôle selon la revendication 1.

Selon l'invention, lorsqu'une transaction entre la carte et un terminal est lancée, qui utilise au moins une session d'authentification par la carte, le compteur de contrôle est décrémenté d'une unité. Il n'est ré-incrémenté de cette unité que si l'authentification est réussie. Ou bien, le compteur de contrôle est incrémenté d'une unité et n'est ensuite décrémenté de cette unité que si la session d'authentification est réussie.

De préférence, on utilise un compteur de contrôle par clé et/ou par couple de clés de cryptage utilisés dans la carte.

Le compteur de contrôle selon l'invention peut décompter depuis, ou compter jusqu'à une valeur de blocage N représentative du nombre d'échecs autorisés.

Cette valeur de blocage N dépend du type de transactions dans lesquelles la clé ou le couple de clés associé est utilisé. Cette valeur correspond à un

nombre de fois autorisé de transactions échouées ou avortées. Elle tient notamment compte du niveau de sécurité à associer à la transaction, c'est à dire du risque encouru par une fraude sur cette clé ou ce couple de clés.

Par exemple, s'agissant pour une carte de type porte-monnaie électronique, d'une transaction de mise à jour de paramètres de la carte, ces paramètres pouvant être la date d'expiration, les valeurs même des clés, un montant maximum pour une transaction ..., on prévoit une valeur N assez faible, car un très fort degré de sécurité doit être associé à une telle transaction et peu d'erreurs d'utilisation peuvent survenir pour ce type de transaction. S'agissant d'opérations d'achats ou d'annulation d'achats, pour lesquels un certain nombre d'incidents lors de l'utilisation "normale" de la carte peuvent intervenir, dûs notamment à des erreurs d'utilisation par le titulaire, on prévoit une valeur plus grande.

Pour une clé donnée ou un couple de clés donné, lorsque le compteur a atteint sa valeur limite, zéro par décrémentation ou N par incrémentation, l'utilisation de la clé ou du couple de clés est bloquée : aucune transaction utilisant cette clé ou ce couple de clés ne peut plus être effectuée. De préférence, on prévoit que ce blocage est irréversible. On peut cependant prévoir de ré-initialisiser le compteur dans le cas ou un blocage résulte indiscutablement d'une erreur non intentionnelle de l'utilisateur. On peut aussi prévoir de pouvoir modifier la valeur de blocage N, si elle se révèle en pratique trop faible ou trop grande. Ces ré-initialisation ou modification ne pourront se faire que selon une procédure très sécurisée par un tiers habilité (la banque).

En outre, dans certaines transactions, plusieurs calculs cryptographiques sont exécutés, avec la même clé ou le même couple de clés jusqu'à et y compris celui de la session d'authentification par la carte. On prévoit alors de décrémenter, ou incrémenter, le compteur ou bien d'une nouvelle unité avant chaque calcul, ou bien d'une unité représentative du nombre de calculs effectués. Si la session d'authentification est réussie, le compteur est ré-incrémenté, ou décrémenté, soit de la somme des unités décrémentées, ou incrémentées, au moyen d'un compteur de pointage ou de l'unité représentative, selon le mode d'implémentation choisi du procédé de contrôle selon l'invention.

D'autres caractéristiques et avantages de l'invention sont décrits dans la description suivante, faite à titre indicatif et nullement limitatif et en référence aux dessins annexés dans lesquels :

- la figure 1 déjà décrite représente un schéma type de calculs cryptographiques effectués lors d'une transaction entre une carte de type porte-monnaie électronique utilisant un algorithme de cryptographie à clé secrète et un terminal;

- la figure 2 est un schéma général des ressources d'une carte de ce type, comprenant des compteurs de contrôle selon l'invention; et

- les figures 3 à 5 sont des organigrammes de transactions typiques dans une application porte-monnaie électronique mettant en oeuvre le procédé de contrôle d'utilisation selon l'invention.

Le principe général de l'invention est d'utiliser au moins un compteur de contrôle que l'on va décrémenter, ou incrémenter d'une unité en début de transaction entre un terminal et une carte, et que l'on ne va ré-incrémenter, ou décrémenter qu'après une session d'authentification par la carte, si cette session est réussie.

Dans la suite on ne retient que le cas ou le compteur est décrémenté systématiquement au début de chaque transaction et ré-incrémenté sous conditions. On se transposera aisément dans le cas inverse ou le compteur est incrémenté systématiquement, en début de transaction, et décrémenté sous conditions.

Le compteur est initialisé à une valeur de blocage N, représentative du nombre d'échecs autorisés qui est notamment fonction de l'application. Si beaucoup de transactions sont démarrées sans permettre une authentification réussie par la carte, soit que la transaction ait été interrompue (cas de *pull out)*, soit que les données envoyées à la carte pour permettre l'authentification par la carte soient fausses (cas d'un simulateur utilisé à la place d'un vrai terminal), le compteur qui est décrémenté à chaque nouvelle transaction, mais qui n'est pas ré-incrémenté dans tous les cas d'échecs d'authentification par la carte, finit par atteindre zéro. L'utilisation de la carte est alors bloquée.

Un exemple de mise en oeuvre de l'invention va maintenant être expliqué pour une carte de type porte-monnaie électronique mettant en oeuvre un algorithme de cryptographie dont la clé de cryptage est une clé secrète. L'invention ne se limite pas ni à ce type de carte, ni à ce type d'algorithme. Elle s'applique à toute carte effectuant pour au moins une transaction, une session d'authentification. La session d'authentification peut utiliser un algorithme à clé secrète comme l'algorithme DES, ou un algorithme de type RSA utilisant un couple de clés de cryptage (clé privée, clé publique). Certaines cartes implémentent même ces deux algorithmes pour utiliser l'un ou l'autre selon la transaction à effectuer. Le procédé de contrôle selon l'invention s'applique à toutes ces différentes cartes et applications.

La figure 2 représente schématiquement les ressources d'une carte à puce de type porte-monnaie électronique, à laquelle on peut appliquer le procédé de contrôle de l'invention.

Elle comprend principalement un microprocesseur µP, et des ressources mémoires dont une mémoire morte ROM, contenant en pratique le code programme, une mémoire dynamique RAM comme mémoire de travail et une mémoire non volatile de type EEPROM par exemple, qui contient en pratique des paramètres sensibles (au sens sécurité) de la carte, dont des compteurs. Dans l'exemple, cette mémoire contient notamment trois clés secrètes notées KDP, KDL et KDU, trois compteurs de sessions associés, notés NTP, NTL et NTU, et trois compteurs de contrôle associés selon l'invention, notés C_{KDP}, C_{KDL}, C_{KDU}.

Cette mémoire contient d'autres paramètres. Certains peuvent être mis à jour par un système externe, par une transaction de mise à jour, selon une procédure sécurisée.

On rappelle que dans une carte porte-monnaie électronique, trois types de transactions sont possibles et à chaque type de transaction correspond une clé secrète associée. On a ainsi les types de transaction suivants :

- Achat ou annulation d'achat (*purchase or purchase cancellation*) avec la clé secrète associée, notée KDP;
- Chargement ou déchargement (*Load or Unload*) avec la clé secrète associée, noté KDL et
- Mise à jour (*update*) avec la clé secrète associée, notée KDU.

Dans l'invention, on prévoit alors d'utiliser un compteur de contrôle par clé secrète différente. On a ainsi le compteur CKDP associé à la clé secrète KDP, le compteur CKDL associé à la clé secrète KDL et le compteur CKDU associé à la clé secrète KDU.

L'exemple d'organigramme de fonctionnement d'une telle carte représenté sur la figure 3 concerne une transaction de type achat (*purchase*), pour laquelle la carte utilise donc la clé secrète KDP, le compteur de session associé NTP et le compteur de contrôle associé selon l'invention, C_{KDP}.

Une transaction d'achat comprend une première phase d'initialisation qui se limite normalement à l'envoi d'une commande par le terminal à la carte, pour lui spécifier le type de transaction. On libelle habituellement cette commande de la manière suivante, dans la littérature anglo-saxonne : *INIT FOR PURCHASE*.

Le microprocesseur se branche alors sur l'adresse du code programme correspondant à ce type de transaction.

Dans l'invention, on prévoit dans cette phase d'initialisation de décrémenter le compteur de contrôle concerné, C_{KDP}, d'une unité. La carte exécute donc l'instruction suivante : $C_{KDP} = C_{KDP} - u$.

Elle teste alors si le compteur de contrôle a atteint sa valeur limite, dans l'exemple zéro. Si il a atteint sa valeur limite ($C_{KDP} \leq 0$), la carte ne peut donner suite à la transaction, qui se terminera donc par défaut de réponse par la carte.

Si la limite n'est pas atteinte, la carte passe à une phase de traitement, dans laquelle elle procède notamment aux opérations suivantes :

- elle calcule la clé de session SK_p, en appliquant l'algorithme de cryptographie à la valeur du compteur de session NTP et en utilisant la clé secrète KDP,
- elle envoie une donnée au terminal pour qu'il calcule une signature correspondante $S2_T$,
- elle reçoit en retour la signature $S2_T$ calculée par le terminal,

- elle calcule une signature S2 en appliquant l'algorithme de cryptographie à la donnée variable envoyée au terminal, avec la clé de session SK_p.

La carte compare alors les deux signatures. Si elles sont comparables, l'authentification est réussie, le compteur de contrôle selon l'invention est alors ré-incrémenté par la valeur u. Sinon, il est inchangé. La transaction peut ensuite continuer.

On voit que si trop de transactions de type achat conduisent à un échec de l'authentification par la carte, le compteur de contrôle selon l'invention va permettre de bloquer toute utilisation de la carte pour une transaction de type achat.

En fait il bloque toute utilisation de la carte pour des transactions de même type, utilisant la même clé secrète. Ainsi, dans le cas du compteur C_{KDP}, ce sont les transactions d'achat ou d'annulation d'achat qui seront bloquées.

La figure 4 montre un organigramme de fonctionnement de la carte pour la transaction de type annulation d'achat, qui utilise donc la même clé secrète KDP.

Dans cette transaction, la phase d'initialisation initiée par une commande d'initialisation du terminal, (commande "*init for purchase cancellation*" selon la littérature anglo-saxonne), comprend, en plus de la décrémentation d'une unité u du compteur de contrôle C_{KDP} selon l'invention, le calcul de la clé de session SK_p et d'une signature S1 obtenue par application d'un algorithme de cryptographie sur une donnée, en utilisant la clé de session. A l'issue de ce calcul, la carte transmet au terminal, cette donnée et la signature S1, pour permettre au terminal d'authentifier la carte. Cette authentification par le terminal ne fait l'objet d'aucune réponse du terminal.

La carte passe à la phase de traitement dans laquelle elle authentifie à son tour le terminal, comme précédemment. Dans ce type de transaction, la signature S2 est en général calculée sur zéro. La carte calcule donc la signature S2 correspondante avec la clé de session KDP. Elle reçoit la signature $S2_T$ calculée par le terminal et effectue la comparaison des deux signatures. Si elles sont comparables, la session d'authentification est réussie. Le compteur de contrôle selon l'invention est ré-incrémenté par l'unité u. Sinon, le compteur de contrôle est inchangé. La transaction se poursuit.

Dans le cas de cette transaction, on voit que la carte effectue deux calculs cryptographiques jusqu'à et y compris celui de la session d'authentification par la carte, le calcul de la signature S1 et le calcul de la signature S2. Pour cette transaction, on prévoit alors de préférence de décrémenter le compteur de contrôle d'une valeur correspondant au nombre de calculs cryptographiques effectués jusqu'à et y compris celui de la session d'authentification par la carte.

Cette décrémentation peut se faire en une seule fois, par une unité u représentative de ce nombre de calculs réalisés pour cette transaction. La valeur prise par u pour cette transaction pourrait être initialisée dans la phase d'initialisation, suite à la commande du type "*INIT FOR*". Cette décrémentation en plusieurs fois, en décrémentant d'une unité le compteur avant chaque calcul, dans l'exemple, avant le calcul de la signature S1 et avant le calcul de la signature S2. Dans ce cas, on prévoira de faire le test de la valeur limite sur le compteur après chaque décrémentation.

Dans ce cas aussi, on prévoit alors un compteur de pointage associé au compteur de contrôle, noté D_{KDP} sur la figure 2, initialisé à zéro au début de la transaction et que l'on vient par exemple incrémenter à

chaque fois que l'on décrémente le compteur de contrôle. Ainsi, si l'authentification par la carte est réussie, on ré-incrémente le compteur de contrôle du nombre contenu dans le compteur de pointage.

On notera que l'homme du métier utilisera l'une ou l'autre des différentes possibilités de mise en oeuvre selon les spécificités de l'application visée. Notamment on peut utiliser une mise en oeuvre pour un type de transactions et une autre pour un autre type de transactions selon le degré de sécurité voulu.

La figure 5 représente un organigramme de fonctionnement pour une autre type de transaction, celle de mise à jour. Il est relativement semblable aux précédents, mais l'authentification par la carte se fait ici sur la signature notée S1.

En fait, de manière générale, le compteur de contrôle est décrémenté au début de la transaction. Il n'est ré-incrémenté, s'il peut l'être, qu'après une session d'authentification par la carte.

On notera que les organigrammes des figures 3 à 5 ne montrent que certaines des opérations effectuées au cours de la transaction, pour l'explication du procédé selon l'invention. En pratique, d'autres opérations sont exécutées. Notamment selon les transactions, on utilise pour calculer les signatures la clé de session courante, ou la clé de session précédente. Après le calcul de la clé de session, le compteur de session doit-être incrémenté ... Tous ces aspects sont spécifiques de l'application à proprement parler et n'ont pas d'intérêt quant à la mise en oeuvre du procédé de contrôle selon l'invention.

Les différents compteurs de contrôle doivent être initialisés à une valeur de blocage N bien choisie. Cette valeur doit tenir compte du type de transactions associé, du niveau de sécurité correspondant à mettre en oeuvre mais aussi des erreurs possibles en cours

d'utilisation "normale" par le titulaire de la carte : il ne s'agit pas de bloquer l'utilisation de la carte alors que le titulaire n'a pas cherché à faire une fraude.

Dans un exemple à titre purement illustratif, mais qui rend compte des différents aspects qui doivent être pris en compte, on peut initialiser le compteur de contrôle C_{KDP} associé aux transactions achat/annulation d'achat à 100, le compteur de contrôle C_{KDL} associé aux transactions chargement/déchargement à 20, et le compteur de contrôle $C_{KD}u$ associé aux transactions de mise à jour à 10.

On a expliqué précédemment qu'une variante du procédé de contrôle selon l'invention consiste à incrémenter le compteur à chaque session et à ne le décrémenter que sous condition (authentification par la carte réussie). Dans ce cas, le compteur est initialisé à zéro, et la valeur limite, à laquelle le contenu du compteur est comparé, est égale à la valeur de blocage N. Tout ce qui a été décrit précèdemment s'applique à cette variante de l'invention.

L'invention vient d'être expliquée dans un exemple d'application à une carte porte-monnaie électronique. Mais il ressort clairement de cette description que le procédé de contrôle selon l'invention s'applique à tout type de carte à puce dès lors qu'elle réalise une session d'authentification. Cette session d'authentification peut être basée sur un algorithme de cryptographie à clé secrète, par exemple de type DES, comme expliqué dans le cas de la carte porte-monnaie électronique, mais aussi des algorithmes d'autres type, comme les algorithmes de type RSA utilisant un couple de clés (clé privée, clé publique) par exemple. Par ailleurs, dans l'invention, on entend par carte à puce aussi bien les cartes de format bien connu que des supports portables.

REVENDICATIONS

1. Procédé de contrôle de l'utilisation d'une carte à puce comprenant un microprocesseur apte à effectuer des calculs de cryptographie dans la carte pour effectuer des sessions d'authentification lors d'une transaction entre la carte et un terminal, caractérisé en ce que ledit procédé utilise au moins un compteur de contrôle (C_{KDP}) et en ce que pour une transaction comprenant au moins une session d'authentification par la carte, le procédé consiste :

- à décrémenter, ou incrémenter, d'une unité (u) le compteur de contrôle au début de la transaction et
- si l'authentification par la carte est réussie, à effectuer la ré-incrémentation, ou la décrémentation, dudit compteur de contrôle par ladite unité (u).

2. Procédé selon la revendication 2, caractérisé en ce que le compteur de contrôle peut décompter depuis, ou compter jusqu'à, une valeur de blocage.

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend l'utilisation d'un compteur de contrôle par clé et/ou par couple de clés de cryptage contenus dans la carte.

4. Procédé selon la revendication 3, caractérisé en la valeur de blocage associée à un compteur est fonction du type de transactions dans lesquelles la clé associée ou le couple de clés associé est utilisé.

5. Procédé selon la revendication 3, caractérisé en ce que l'unité de décrémentation, ou d'incrémentation, d'un compteur de contrôle est représentative du nombre de calculs cryptographiques avec la clé associée ou le

couple de clés associé, effectués jusqu'à et y compris celui de ladite session d'authentification pendant ladite transaction.

6. Procédé selon la revendication 3, caractérisé en ce que le compteur de contrôle associé à une clé ou un couple de clés est décrémenté, ou incrémenté, d'une nouvelle unité, avant chacun des calculs cryptographiques utilisant ladite clé ou le dit couple de clés, jusqu'à et y compris celui de ladite session d'authentification par la carte.

7. Procédé selon la revendication 5, caractérisé en ce que la ré-incrémentation, ou la décrémentation, du compteur par l'unité représentative du nombre de calculs cryptographiques est effectuée si la session d'authentification par la carte est réussie.

8. Procédé selon la revendication 6, caractérisé en ce qu'il comprend un compteur de pointage (D_{KDP}) pour mémoriser le nombre de décrémentations, ou d'incrémentations, d'une unité effectuées, pour permettre la ré-incrémentation, ou la décrémentation, du compteur de contrôle (C_{KDP}) par le contenu du compteur de pointage, si la session d'authentification par la carte est réussie.

9. Procédé de contrôle selon l'une quelconque des revendications précédentes, caractérisé en ce que ladite session d'authentification par la carte est effectuée lors d'une connexion par liaison directe à un serveur.

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que, lorsque le compteur de contrôle est décrémenté, ou

incrémenté, jusqu'à une valeur limite, il bloque l'utilisation de la clé associée ou du couple de clé associé.

11. Procédé selon la revendication 10, caractérisé en ce que le blocage de l'utilisation de la clé ou du couple de clés est irréversible.

12. Carte à puce comprenant au moins un compteur de contrôle associé à au moins une clé et/ou un couple de clés pour la mise en oeuvre d'un procédé de contrôle selon l'une quelconque des revendications précédentes.

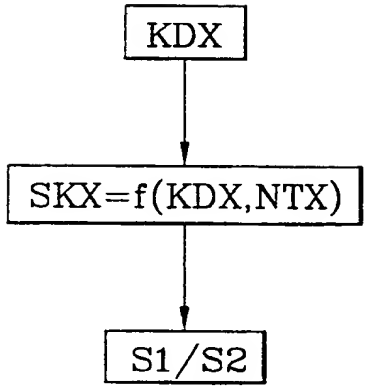

KDX
SKX=f(KDX,NTX)
S1/S2

FIG.1

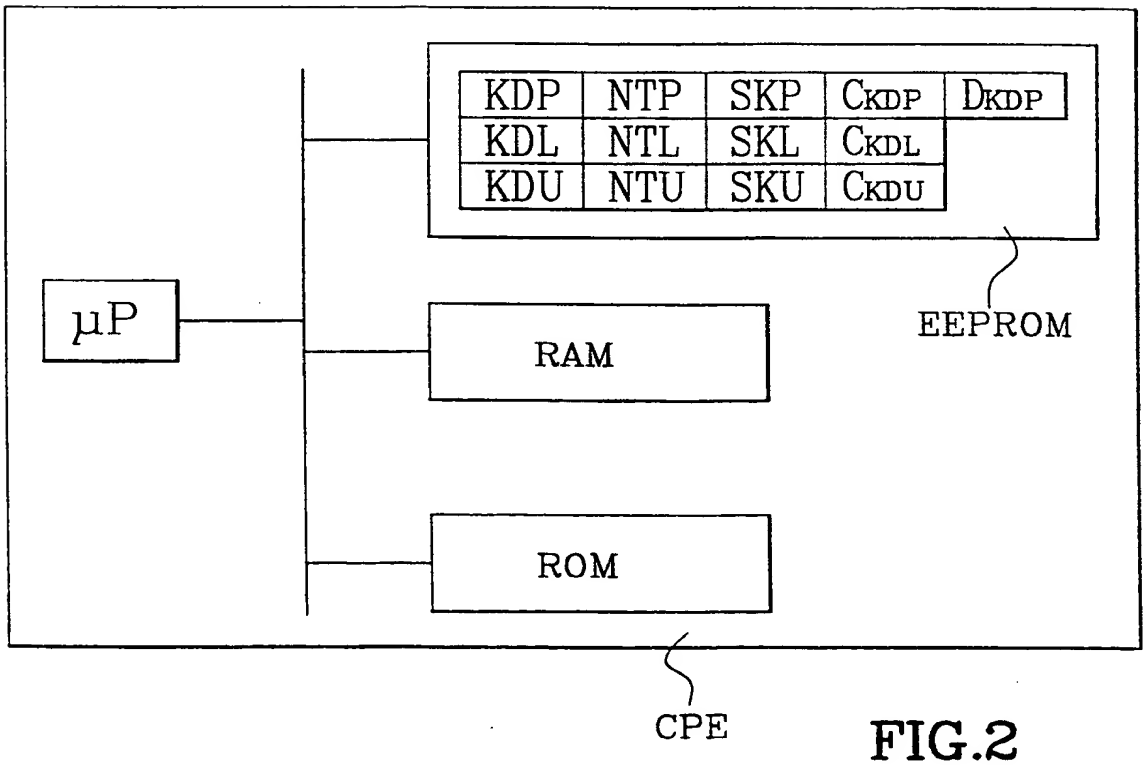

KDP
NTP
SKP
CKDP
DKDP
KDL
NTL
SKL
CKDL
KDU
NTU
SKU
CKDU
EEPROM
µP
RAM
ROM
CPE

FIG.2

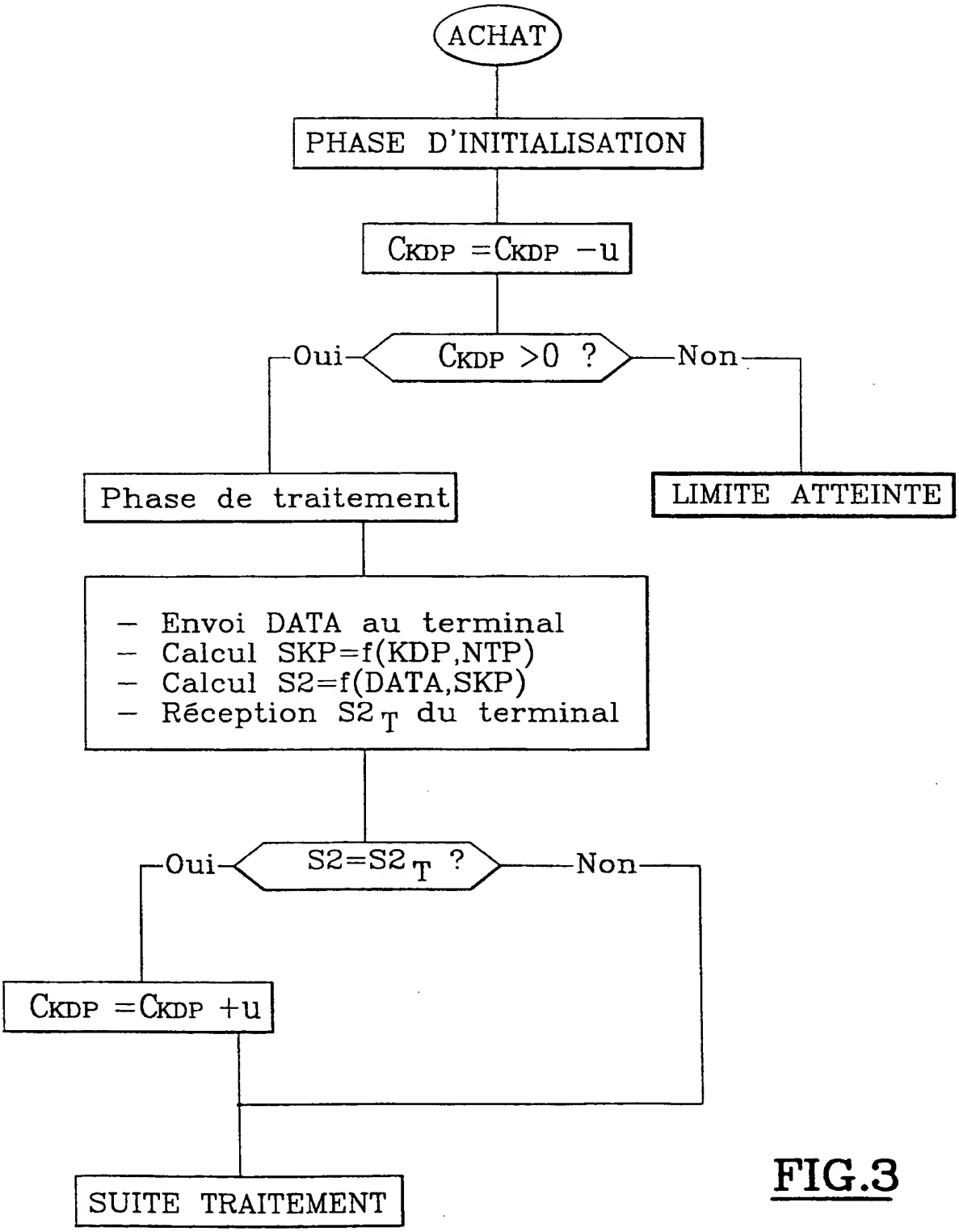

ACHAT
PHASE D'INITIALISATION
CKDP =CKDP -u
Oui
CKDP >0 ?
Non
Phase de traitement
LIMITE ATTEINTE
- Envoi DATA au terminal
- Calcul SKP=f(KDP,NTP)
- Calcul S2=f(DATA,SKP)
- Réception S2T du terminal
Oui
S2=S2T ?
Non
CKDP =CKDP +u
SUITE TRAITEMENT

FIG.3

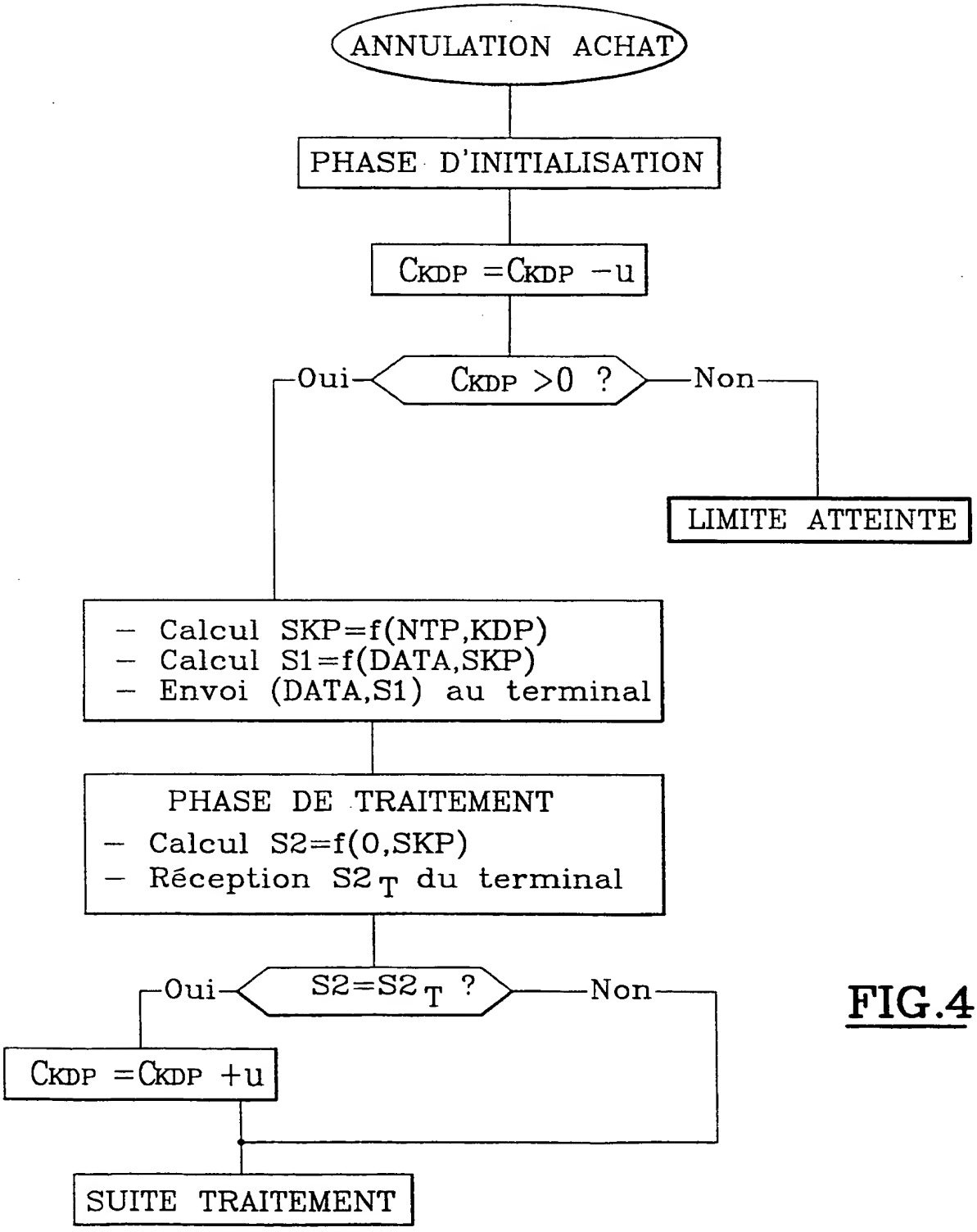

ANNULATION ACHAT
PHASE D'INITIALISATION
CKDP =CKDP -u
Oui
CKDP >0 ?
Non
LIMITE ATTEINTE
- Calcul SKP=f(NTP,KDP)
- Calcul S1=f(DATA,SKP)
- Envoi (DATA,S1) au terminal
PHASE DE TRAITEMENT
- Calcul S2=f(0,SKP)
- Réception S2T du terminal
Oui
S2=S2T ?
Non
CKDP =CKDP +u
SUITE TRAITEMENT

FIG.4

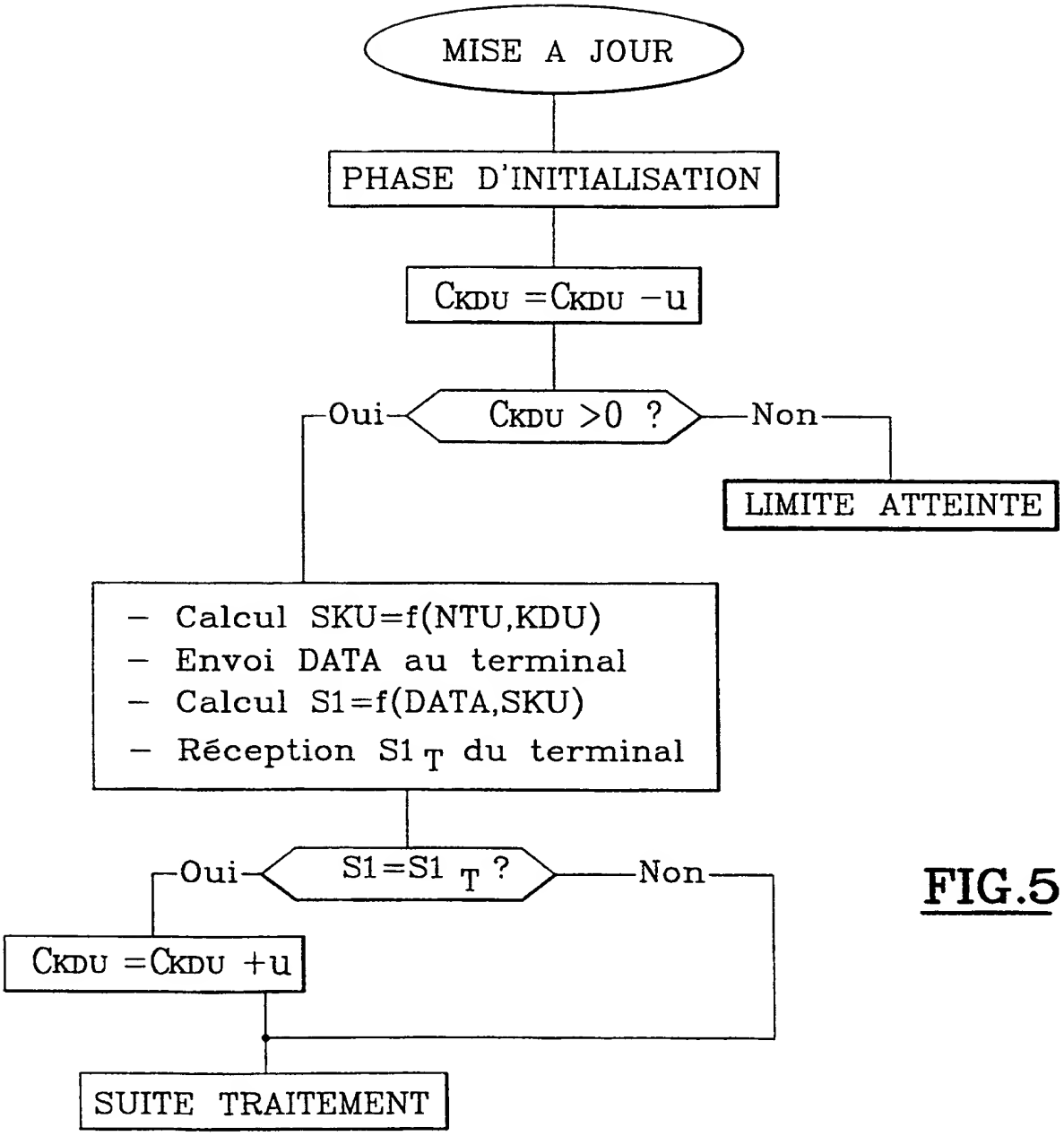

MISE A JOUR
PHASE D'INITIALISATION
CKDU =CKDU -u
Oui
CKDU >0 ?
Non
LIMITE ATTEINTE
- Calcul SKU=f(NTU,KDU)
- Envoi DATA au terminal
- Calcul S1=f(DATA,SKU)
- Réception S1 T du terminal
Oui
S1=S1 T ?
Non
CKDU =CKDU +u
SUITE TRAITEMENT

FIG.5

INTERNATIONAL SEARCH REPORT

Application No
PCT/FR 99/02782

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 789 335 A (DEUTSCHE TELEKOM) 13 August 1997 (1997-08-13)	1,2
A	the whole document	9
Y	EP 0 481 882 A (GEMPLUS CARD INTERNATIONAL) 22 April 1992 (1992-04-22) abstract; claims; figures	1,2
A	GB 2 188 762 A (P.H. BERTENSHAW) 7 October 1987 (1987-10-07) the whole document	1-5,9-11
A	EP 0 626 662 A (GEMPLUS CARD INTERNATIONAL) 30 November 1994 (1994-11-30)	
A	EP 0 157 303 A (TOSHIBA) 9 October 1985 (1985-10-09)	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 February 2000	06/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

National Application No
PCT/FR 99/02782

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0789335 A	13-08-1997	DE 19604349 A	14-08-1997
EP 0481882 A	22-04-1992	FR 2668278 A	24-04-1992
		CA 2053740 A,C	20-04-1992
		DE 69101099 D	10-03-1994
		DE 69101099 T	07-07-1994
		ES 2059085 T	01-11-1994
		JP 4264688 A	21-09-1992
		JP 7066431 B	19-07-1995
		US 5296687 A	22-03-1994
GB 2188762 A	07-10-1987	NONE	
EP 0626662 A	30-11-1994	FR 2705810 A	02-12-1994
		DE 69419967 D	16-09-1999
		DE 69419967 T	09-12-1999
		US 5550919 A	27-08-1996
EP 0157303 A	09-10-1985	JP 60207957 A	19-10-1985
		US 4879645 A	07-11-1989

RAPPORT DE RECHEI E INTERNATIONALE

D ternationale No
PCT/FR 99/02782

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 789 335 A (DEUTSCHE TELEKOM) 13 août 1997 (1997-08-13)	1,2
A	le document en entier	9
Y	EP 0 481 882 A (GEMPLUS CARD INTERNATIONAL) 22 avril 1992 (1992-04-22) abrégé; revendications; figures	1,2
A	GB 2 188 762 A (P.H. BERTENSHAW) 7 octobre 1987 (1987-10-07) le document en entier	1-5,9-11
A	EP 0 626 662 A (GEMPLUS CARD INTERNATIONAL) 30 novembre 1994 (1994-11-30)	
A	EP 0 157 303 A (TOSHIBA) 9 octobre 1985 (1985-10-09)	

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents citées:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 février 2000	06/03/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

de internationale No
PCT/FR 99/02782

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0789335	A	13-08-1997	DE 19604349	A	14-08-1997
EP 0481882	A	22-04-1992	FR 2668278	A	24-04-1992
			CA 2053740	A,C	20-04-1992
			DE 69101099	D	10-03-1994
			DE 69101099	T	07-07-1994
			ES 2059085	T	01-11-1994
			JP 4264688	A	21-09-1992
			JP 7066431	B	19-07-1995
			US 5296687	A	22-03-1994
GB 2188762	A	07-10-1987	AUCUN		
EP 0626662	A	30-11-1994	FR 2705810	A	02-12-1994
			DE 69419967	D	16-09-1999
			DE 69419967	T	09-12-1999
			US 5550919	A	27-08-1996
EP 0157303	A	09-10-1985	JP 60207957	A	19-10-1985
			US 4879645	A	07-11-1989